

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

10/18/2019

**SUBJECT:**

Multiple Vulnerabilities in Cisco Products Could Allow for Remote Unauthorized Access with Elevated Privileges

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for remote unauthorized access with elevated privileges on the affected system. For affected access points, an attacker could view sensitive information, update the network configuration, and disable the access point resulting in a denial of service.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- Aironet 1540 Series APs
- Aironet 1560 Series APs
- Aironet 1800 Series APs
- Aironet 1810 Series APs
- Aironet 1830 Series APs
- Aironet 1850 Series Aps
- Aironet 2800 Series APs
- Aironet 3800 Series APs
- Aironet 4800 APs
- Aironet 9100 APs
- Firepower Management Center (FMC) Software
- FMC Software releases earlier than Release 6.5.0
- Wireless LAN Controller (WLC) Software releases 8.5.140.0 and earlier
- Wireless LAN Controller (WLC) Software releases earlier than Release 8.10
- SPA112 2-Port Phone Adapter and SPA122 ATA with Router devices that are running firmware releases 1.4.1 SR4 and earlier and that have the web-based management interface enabled.
- 250 Series Smart Switches
- 350 Series Managed Switches
- 550X Series Stackable Managed Switches
- Expressway Series and TelePresence VCS running a software release earlier than Release X12.5.4

- TelePresence CE Software releases earlier than Release 9.8.0
- TelePresence CE Software releases earlier than Release 9.8.1
- SPA100 Series ATAs that were running firmware releases 1.4.1 SR3 and earlier
- Business 200 Series Smart Switches
- Business 300 Series Managed Switches
- Business 500 Series Stackable Managed Switches
- ISE Software releases earlier than Release 2.4.0 Patch 10
- ISE releases earlier than 2.4P10 or 2.3P7
- FindIT Network Probe versions 1.0.0 and 1.0.1

#### **RISK:**

##### **Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

##### **Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

##### **Home Users: Low**

#### **TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow a remote, unauthenticated attacker, unauthorized access with elevated privileges on the affected system. Details of these vulnerabilities are as follows:

- A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. (CVE-2019-12687, CVE-2019-12688).
- A vulnerability in Cisco Aironet Access Points (APs) Software could allow an unauthenticated, remote attacker to gain unauthorized access to a targeted device with elevated privileges. (CVE-2019-15260)
- A vulnerability in the Secure Shell (SSH) session management for Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2019-15262)
- Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. (CVE-2019-15240, CVE-2019-15241, CVE-2019-15242)
- A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. (CVE-2019-12636)
- A vulnerability in the Point-to-Point Tunneling Protocol (PPTP) VPN packet processing functionality in Cisco Aironet Access Points (APs) could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. (CVE-2019-15261)
- A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol implementation of Cisco Aironet and Catalyst 9100 Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. (CVE-2019-15264)
- A vulnerability in the CLI of Cisco Wireless LAN Controller (WLC) Software could allow an authenticated, local attacker to view system files that should be restricted. (CVE-2019-15266)

- A vulnerability in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected system. (CVE-2019-12705)
- A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to execute code with root privileges. (CVE-2019-15277)
- A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. (CVE-2019-15275)
- A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. (CVE-2019-15962)
- Multiple vulnerabilities in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to overwrite arbitrary files. (CVE-2019-15273)
- A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to perform command injections. (CVE-2019-15274)
- A vulnerability in the web-based management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to cause a denial of service condition on an affected device. (CVE-2019-15258)
- A vulnerability in the web-based management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to view the contents of arbitrary files on an affected device. (CVE-2019-12704)
- A vulnerability in the web-based management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to access sensitive information on an affected device. (CVE-2019-15257)
- A vulnerability in the web-based management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to conduct cross-site scripting attacks. (CVE-2019-12702)
- A vulnerability in the web-based management interface of Cisco SPA122 ATA with Router Devices could allow an unauthenticated, adjacent attacker to conduct cross-site scripting attacks. (CVE-2019-12703)
- A vulnerability in the web-based management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to access sensitive information on an affected device. (CVE-2019-12708)
- A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. (CVE-2019-12718)
- A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. (CVE-2019-15281)
- Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web-based management interface. (CVE-2019-12637)
- A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web-based management interface. (CVE-2019-12638)

- A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to read tcpdump files generated on an affected device. (CVE-2019-15282)
- A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface. (CVE-2019-15280)
- Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. (CVE-2019-15268, CVE-2019-15269)
- A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. (CVE-2019-15270)
- A vulnerability in the bridge protocol data unit (BPDU) forwarding functionality of Cisco Aironet Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an AP port to go into an error disabled state. (CVE-2019-15265)
- Multiple Issues in Cisco Small Business 250/350/350X/550X Series Switches Firmware and Cisco FindIT Network Probe (No associated CVEs)

Successful exploitation of the most severe of these vulnerabilities could allow for remote unauthorized access with elevated privileges on the affected system. For affected access points, an attacker could view sensitive information, update the network configuration, and disable the access point resulting in a denial of service.

## **RECOMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Cisco immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

## **REFERENCES:**

### **Cisco:**

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce>

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-airo-unauth-access>

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-wlc-ssh-dos>

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-spa-rce>

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-sbss-csrf>

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-airo-pptp-dos>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-airo-capwap-dos>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-wlc-pathtrav>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-vcs-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-telepres-escalation>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-telece-privescal>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-telece-filewrite>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-telece-file-ovrwr>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-telece-cmdinj>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-spa-webui-dos>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-spa-ui-disclosure>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-spa-running-config>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-spa-reflected-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-spa-dhcp-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-spa-credentials>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-sbss-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-ise-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-ise-stored-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-ise-store-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-ise-infodis>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-fpwr-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-firepwr-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-firepwr-stored-xss>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-airo-dos>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-sb-switches-findit>

**CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12636>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12637>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12638>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12687>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12688>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12702>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12703>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12704>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12705>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12708>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-12718>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15240>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15241>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15242>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15257>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15258>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15260>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15261>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15262>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15264>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15265>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15266>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15268>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15269>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15270>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15273>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15274>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15275>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15277>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15280>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15281>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15282>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE--2019-15962>

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

**<http://www.us-cert.gov/tlp/>**

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

**Chris Watts**  
Security Operations Analyst  
MS Department of Information Technology Services  
601-432-8201 | [www.its.ms.gov](http://www.its.ms.gov)



DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited